UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/567,335	10/10/2006	Ingo Buettner		9376

181 7590 08/04/2009

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
LEWIS-TAYLOR, DAYTON A.	

ART UNIT	PAPER NUMBER
2182	

NOTIFICATION DATE	DELIVERY MODE
08/04/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipdocketing@milesstockbridge.com
sstiles@milesstockbridge.com

Office Action Summary	Application No.	Applicant(s)	
	10/567,335	BUETTNER, INGO	
	Examiner	Art Unit	
	DAYTON LEWIS-TAYLOR	2182	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13,15-17 and 20-36* is/are rejected.

7)☒ Claim(s) *14,18 and 19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 February 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/06/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1 Claims 1 – 36 are pending.

.*Information Disclosure Statement*

2. The information disclosure statement (IDS) submitted on February 6, 2006 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Priority

3. Examiner acknowledges Applicant's claim to priority benefits of Foreign Application Priority Data filed August 6, 2003.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 1-7, 10, 25-27, 30-32 and 35** are rejected under 35 U.S.C. 102(b) as being anticipated by Mooney et al. (5,610,981) hereinafter referred to as Mooney.

As per claim 1, Mooney discloses a monitoring device (1) for a data processing system (2) in a network comprising network connections (4), for protecting data storage and/or data transmission means of the data processing system against unauthorized access, the data processing system comprising a disabling circuit (6) for interfaces (8, 10, 12,

14) ***(Mooney – col. 10, lines 52-60: "Bus address monitor '930' monitors system bus '292' references to peripheral devices such as serial and parallel ports, networks, and A or B floppy disks. Bus address monitor '930' monitors normal BIOS references during initialization, such as reset, warm, or power-up boot, and monitors to detect attempted prohibited accesses to denied peripheral devices as defined on card '115' during the authorization visit.")***,

characterized in

that only a single data storage means (9) is connected to a bootable interface (8) of the data processing system (2) as a mainboot device that can boot freely ***(Mooney – col. 12, line 67 – col. 13, line 4: "At initialization, CPU '290' executes the standard BIOS routine of loading the first "one and/or two sectors" from the C: drive. Card reader interface board '109' intercepts the read issued by CPU '290' and directs it to ROM '280'.")***,

that other bootable interfaces (10, 12, 14) are disabled at first ***(Mooney – col. 15, lines 3-10: "If any unauthorized accesses are attempted, system bus '292' is frozen and the verification program terminates. Unauthorized accesses include: unauthorized access of peripheral and attempts to boot from the A: instead of C: drive")***, and

that at least one of the interfaces (10, 12, 14) disabled by the disabling circuit (6) is enabled from a data processing point (16) located at a distance in the network via the network connection (4) after authorization of an authorized person at the data processing point (16) ***(Mooney – col. 2, lines 57-59: "if the responses match the correct answers, the CPU is allowed to access all peripherals the user has been authorized to use")***.

As per claim 2, Mooney discloses the monitoring device of claim 1, characterized in that the disabling circuit (6) disables the bootable interfaces (10, 12, 14) ***(Mooney – col. 15, lines 3-10: "If any unauthorized accesses are attempted, system bus '292' is frozen and the verification program terminates. Unauthorized accesses include: unauthorized access of peripheral and attempts to boot from the A: instead of C: drive")*** via a CMOS ***(Mooney – col. 4, line 54: "printed circuit board technology")***.

As per claim 3, Mooney discloses the monitoring device of claim 1, characterized in that the disabling circuit (6) is integrated on the motherboard ***(Mooney - col. 6, lines 14-15: "integrated into the motherboard of computer '100'")***.

As per claim 4, Mooney discloses the monitoring device of claim 1, characterized in that the disabling circuit (6) is arranged on a separate card with a separate interface, preferably a PCI card ***(Mooney – col. 4, line 63: "An IC card '115'" and col. 4, lines 46-47: "a card reader interface")***.

As per claim 5, Mooney discloses the monitoring device of claim 1, characterized in that the disabling circuit (6) includes a microcontroller ***(Mooney – col. 5, lines 10-12: "Microprocessor '116' is powered by circuit '135', and controls system functions via connections to the system data bus '125'")***.

As per claim 6, Mooney discloses the monitoring device of claim 1, characterized in that the disabling circuit (6) is controlled by the data processing point (16) through a receiving

line (22) of the network connection (4) ***(Mooney – Fig. 3: "Processor Z8 '220' connected to Data Steering Network '240' via bus '222'")***.

As per claim 7, Mooney discloses the monitoring device of claim 1, characterized in that the disabling circuit (6) comprises a reset line (24), preferably a power reset ***(Mooney – Abstract: "freezing the system bus, and requiring the user to reset the computer")***.

As per claim 10, Mooney discloses the monitoring device of claim 1, characterized in hat at least one plug-in connection for a keyboard and/or a universal serial port of the data processing system (2) is provided with an alarm circuit (38), preferably a socket switch, which is preferably connected to the network connection (4) and is adapted to transmit an alarm signal via the network connection (4) ***(Mooney – Fig. 1A & 1B: Keyboard '101' plugged into computer)***.

As per claim 25, Mooney discloses a method for monitoring a data processing system (2) in a network comprising network connections (4), for protecting data storage and/or data transmission means of the data processing system (2) against unauthorized access ***(Mooney – col. 10, lines 52-60: "Bus address monitor '930' monitors system bus '292' references to peripheral devices such as serial and parallel ports, networks, and A or B floppy disks. Bus address monitor '930' monitors normal BIOS references during initialization, such as reset, warm, or power-up boot, and monitors to detect attempted prohibited accesses to denied peripheral devices as defined on card '115' during the authorization visit.")***,

characterized in

that, upon booting, only a single data storage means can be accessed at a bootable interface (8) of the data processing system (2) ***(Mooney – col. 12, line 67 – col. 13, line 4: "At initialization, CPU '290' executes the standard BIOS routine of loading the first "one and/or two sectors" from the C: drive. Card reader interface board '109' intercepts the read issued by CPU '290' and directs it to ROM '280'.")***,

that other bootable interfaces (10, 12, 14) are disabled at first ***(Mooney – col. 15, lines 3-10: "If any unauthorized accesses are attempted, system bus '292' is frozen and the verification program terminates. Unauthorized accesses include: unauthorized access of peripheral and attempts to boot from the A: instead of C: drive")***, and

that the disabled interfaces (10, 12, 14) are enabled from a data processing point (16) located at a distance in the network via the network connection (4) after authorization of an authorized person at the data processing point (16) ***(Mooney – col. 2, lines 57-59: "if the responses match the correct answers, the CPU is allowed to access all peripherals the user has been authorized to use")***.

As per claim 26, Mooney discloses the method of claim 25, characterized in that the disabling of the interfaces (10, 12, 14) is controlled by the data processing point (16) ***(Mooney – Fig.1: Processor Z8 '280')*** via a receiving line of the network connection (4) ***(Mooney - Fig. 5: Data steering network '240')*** and a disabling circuit (6) ***(Mooney – col. 15, lines 3-10: "If any unauthorized accesses are attempted, system bus '292' is frozen and the verification program terminates. Unauthorized accesses include: unauthorized access of peripheral and attempts to boot from the A: instead of C: drive")***.

As per claim 27, Mooney discloses the method of claim 25, characterized in that the disabling of the bootable interfaces (10, 12, 14) is restored to the disabled state after the data processing system (2) has been switched off and/or after a user has logged off at the data processing system (2) ***(Mooney – col. 9, lines 22-23: "Freeze the computer system bus, requiring a "cold boot," (power off and then on or "reset")")***.

As per claim 30, the method of claim 28, characterized in that a mechanical destruction of at least one access-protected data carrier of the data processing system (2) is caused by an alarm triggered ***(Mooney - col. 16, lines 50-52: "triggering destruct package '213' designed to physically destroy the hard drive '113' and RAM '260'")***.

As per claim 31, Mooney discloses the monitoring device of claim 2, characterized in that the disabling circuit (6) is integrated on the motherboard ***(Mooney - col. 6, lines 14-15: "integrated into the motherboard of computer '100'")***.

As per claim 32, Mooney discloses the monitoring device of claim 2, characterized in that the disabling circuit (6) is arranged on a separate card with a separate interface, preferably a PCI card ***(Mooney – col. 4, line 63: "An IC card '115'" and col. 4, lines 46-47: "a card reader interface")***.

As per claim 35, Mooney discloses the method of claim 26, characterized in that the disabling of the bootable interfaces (10, 12, 14) is restored to the disabled state after the data processing system (2) has been switched off and/or after a user has logged off at

the data processing system (2) ***(Mooney – col. 9, lines 22-23: "Freeze the computer system bus, requiring a "cold boot," (power off and then on or "reset")")***.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

8. **Claims *8-9,*** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of McClung et al. (4,951,249) hereinafter referred to as McClung.

As per claim 8, Mooney discloses the monitoring device of claim 1, and the bootable interface ***(Mooney – col. 12, line 67 – col. 13, line 4: "At initialization, CPU '290'***

executes the standard BIOS routine of loading the first "one and/or two sectors" from the C: drive.").

Mooney does not expressly disclose that monitoring device has an alarm circuit (28, 30, 32, 34) connected to at least one bootable interface (8, 10, 12, 14), said alarm circuit preferably being connected to the network connection (4) being adapted to transmit an alarm signal via the network connection and, further, preferably being connected to a free mass port of the interface (8, 10, 12, 14)

McClung discloses an alarm circuit connected characterized in that an alarm circuit is connected to at least one bootable interface ***(McClung – Fig. 1: Alarm circuits '119' connected to ROM '115' and col. 4, lines 48-49: "The computer system is hard wired to transfer program execution to the BOOTSTRAP code contained in the computer system boot ROM.")***.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to McClung's alarm circuit in Mooney's monitoring device to improve the apparatus with reasonable expectation that this would result in a monitoring device that could sound an alarm if the computer is tilted or a screw is loosened or removed on the housing (McClung - col. 2, lines 61-68).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney and McClung to obtain the invention as specified in claim 8.

As per claim 9, Mooney discloses the monitoring device of claim 1 and a housing of the data processing system ***(Mooney - Fig. 1A: Housing of a computer)***.

Mooney does not expressly disclose that the monitor device has the housing of the data processing system (2) provided with an alarm circuit (36), preferably a key switch, which is preferably connected to the network connection (4) and is adapted to transmit an alarm signal via the network connection (4).

McClung discloses a housing of the data processing system is provided with an alarm circuit ***(McClung – col. 2, lines 61-62: "an alarm for a computer system enclosed in a housing").***

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to McClung's alarm circuit in Mooney's monitoring device to improve the apparatus with reasonable expectation that this would result in a monitoring device that could sound an alarm if the computer is tilted or a screw is loosened or removed on the housing (McClung - col. 2, lines 61-68).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney and McClung to obtain the invention as specified in claim 9.

9. **Claims 11, 20-21 and 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of Svensson et al. (5,926,091) hereinafter referred to as Svensson. **As per claim 11**, Mooney discloses the monitoring device of claim 1 and a network connection ***(Mooney – Data Steering Network '240')***.

Mooney does not expressly disclose that the monitoring device has a network connection (4) protected against unauthorized access, such as pulling off one or a plurality of terminal pins, for example, by means of an alarm circuit.

Svensson discloses a network connection is protected against unauthorized access, such as pulling off one or a plurality of terminal pins, for example, by means of an alarm circuit ***(Svensson – col. 4, lines 43-46: 'an alarm is activated from the alarm unit when one of cables '8' connecting the respective personal computer to the computer network hub is removed")***.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Svensson's network connection protected against unauthorized access in Mooney's monitoring device to improve the apparatus with reasonable expectation that this would result in a monitoring device that could use an alarm device to make it possible to detect whether the network is intact or whether the loading in the network has decreased, which would indicate a failure somewhere in the network (Svensson - col. 1, lines 44-47).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney and Svensson to obtain the invention as specified in claim 11.

As per claim 20, Mooney discloses the monitoring device of claim 1.

Mooney does not expressly disclose that the monitoring device characterized in that one or a plurality of the alarm circuits (28, 30, 32, 34, 36, 38) is connected to a separate line strand (26b) of the network connection (4), preferably to individual lines (4e-h), respectively.

Svensson discloses one or a plurality of the alarm circuits is connected to a separate line strand (26b) of the network connection ***(Svensson - col. 6, lines 12-14: "A special alarm unit ''4 is then coupled, e.g., via cable '32', between the network***

connection of the computer unit and its network board '30', as illustrated in FIG. 1.").

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Svensson's alarm circuit connected to a network connection in Mooney's monitoring device to improve the apparatus with reasonable expectation that this would result in a monitoring device that could use an alarm device to detect whether the network is intact or whether the loading in the network has decreased, which would indicate a failure somewhere in the network (Svensson - col. 1, lines 44-47).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney and Svensson to obtain the invention as specified in claim 20.

As per claim 21, Mooney and Svensson disclose the monitoring device of claim 20, and an alarm detection means (46) is connected, remote from the data processing system (2), to the individual lines (4e-h) of the separate line strand (26b) of the network connection (4) ***(Svensson – Fig. 7: Alarm Center '1' is connected, remote from the PC '13a', to the individual line coupled to Hub '3' to individual line toward Network Board '30')***.

As per claim 28, Mooney discloses the method of claim 25.

Mooney does not expressly disclose an alarm is triggered at a remote alarm detection means (46) by removal of a data storage means and/or of a data transmission means of the data processing system (2), as well as by opening a housing of the data processing system (2).

Svensson discloses an alarm is triggered at a remote alarm detection ***(Svensson – Fig. 7: Alarm Center '1')*** means by removal of a data storage means and/or of a data transmission means of the data processing system ***(Svensson – col. 4, lines 43-46: 'an alarm is activated from the alarm unit when one of cables '8' connecting the respective personal computer to the computer network hub is removed")***, as well as by opening a housing of the data processing system ***(Svensson – col. 2, lines 50-53: "the first alarm unit arranged in the computer unit is included in an alarm circuit, which is arranged to be affected on unauthorized opening of the case, whereby the alarm unit is arranged to notify the alarm center")***.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Svensson's alarm circuit connected to a network connection in Mooney's monitoring device to improve the apparatus with reasonable expectation that this would result in a monitoring device that could use an alarm device to detect whether the network is intact or whether the loading in the network has decreased, which would indicate a failure somewhere in the network (Svensson - col. 1, lines 44-47).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney and Svensson to obtain the invention as specified in claim 28.

10. **Claims *12,*** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney, in view of McClung, and further in view of Svensson.

As per claim 12, note that Mooney and McClung disclose the monitoring device of claim 8.

Mooney does not expressly disclose that the monitoring device characterized in that one or a plurality of the alarm circuits (28, 30, 32, 34, 36, 38) is connected to a transmission/receiving line strand (26b) of the network connection (4), preferably to individual lines (4e-h), respectively.

Svensson discloses one or a plurality of the alarm circuits is connected to a transmission/receiving line strand of the network connection ***(Svensson - col. 6, lines 12-14: "A special alarm unit ''4 is then coupled, e.g., via cable '32', between the network connection of the computer unit and its network board '30', as illustrated in FIG. 1.")***.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Svensson's alarm circuit connected to a network connection in Mooney and McClung's monitoring device to improve the apparatus with reasonable expectation that this would result in a monitoring device that could use an alarm device to detect whether the network is intact or whether the loading in the network has decreased, which would indicate a failure somewhere in the network (Svensson - col. 1, lines 44-47).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney, McClung and Svensson to obtain the invention as specified in claim 12.

11. **Claim *13*** is rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of McClung, in view of Svensson, as applied to claim 12, and further in view of Copeland (4,675,654) hereinafter referred to as Copeland.

As per claim 13, note that Mooney, McClung and Svensson disclose the monitoring device of claim 12.

Mooney, McClung and Svensson do not expressly disclose that the monitoring device has alarm circuits (28, 30, 32, 34, 36, 38) connected in parallel through resistors (40) and are combined to one line (42).

Copeland discloses alarm circuits connected in parallel through resistors and are combined to one line ***(Copeland – Fig. 1, col. 4, lines 25-26: "Alarm circuits '16a-h' are all identical alarm circuits connected in parallel" through resistors '38a-h' combined to line '24')***.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Copeland's parallel alarm circuits in Mooney, McClung and Svensson's monitoring device to improve the apparatus with reasonable expectation that this would result in a monitoring device that could use parallel circuits to prevent electrical feedback in the system fro causing false alarm indications (Copeland - Abstract).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney, McClung, Svensson and Copeland to obtain the invention as specified in claim 13.

12. **Claims *15-16*** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of McClung, further in view of Bloom et al. (6,194,979) hereinafter referred to as Bloom, and further in view of Trucchi et al. (6,081,193) hereinafter referred to as Trucchi. **As per claim 15**, note that Mooney and McClung disclose the monitoring device of claim 8, and the network connection ***(Mooney – Fig. 3: Data Steering Network '240')***.

Mooney and McClung do not expressly disclose the monitoring device with at least two capacitors (50) provided in individual lines (4a-d) of the network connection, respectively.

Bloom discloses at least two capacitors ***(Bloom - col. 8, lines 47-50: "As shown in Fig. 9, the capacitors and resistors are arranged in what is know of in the electrical art as a "Y" configuration or star configuration.")***.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Bloom's two capacitors in Mooney and McClung's monitoring device to improve the apparatus with reasonable expectation that this would result in a monitoring device that uses at least two capacitors to regulate power due to the sudden demand for current when an alarm circuit is switching between states.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney, McClung and Bloom to obtain the invention as specified in claim 15.

Mooney, McClung and Bloom do not expressly disclose the monitoring device with individual lines (4a-d) of the network connection.

Trucchi discloses individual lines ***(Trucchi - Fig. 1: Alarm circuits 10a, 10b, 10c are connected to signal transmission lines 14a, 14b, 14c),*** respectively.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Trucchi's individual lines in Mooney, McClung and Bloom's monitoring device having at least two capacitors provided to improve the apparatus with reasonable expectation that this would result in a monitoring device that uses individual lines so that in case of a malfunction of one alarm circuit the rest of alarm circuits would be able to transmit a signal through the network connection.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney, McClung, Bloom and Trucchi to obtain the invention as specified in claim 15.

As per claim 16, note that Mooney, McClung, Bloom and Trucchi disclose the monitoring device of claim 15, and the alarm circuits (28, 30, 32, 34, 36, 38) are connected to the individual lines (4a-d) ***(Trucchi - Fig. 1: Alarm circuits 10a, 10b, 10c are connected to signal transmission lines 14a, 14b, 14c)*** of the network connection (4) ***(Mooney – Fig. 3: Data Steering Network '240')*** by a star wiring between the capacitors (50) ***(Bloom - col. 8, lines 47-50: "As shown in Fig. 9, the capacitors and resistors are arranged in what is know of in the electrical art as a "Y" configuration or star configuration.")***.

13. **Claims 17 and 33** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of McClung, in view of Bloom, in view of Trucchi, and further in view of Svensson.

As per claim 17, note that Mooney, McClung, Bloom and Trucchi disclose the monitoring device of claim 15 and a star wiring between the capacitors (50) ***(Bloom - col. 8, lines 47-50: "As shown in Fig. 9, the capacitors and resistors are arranged in what is know of in the electrical art as a "Y" configuration or star configuration.")***.

Mooney, McClung, Bloom and Trucchi do not expressly disclose the monitoring device with the alarm detection means (46) is connected, remote from the data

processing system (2), to the individual lines (4a-d) of the network connection (4) by a star wiring between the capacitors (50).

Svensson discloses an alarm detection means is connected, remote from the data processing system, to the individual lines of the network connection ***(Svensson – Fig. 7: Alarm Center '1' is connected, remote from the PC '13a', to the individual line coupled to Hub '3' to individual line toward Network Board '30')***.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Svensson's alarm detection connected to a network connection in Mooney, McClung, Bloom and Trucchi's monitoring device with a star wiring between the capacitors to improve the apparatus with reasonable expectation that this would result in a monitoring device that could use an alarm device to detect whether the network is intact or whether the loading in the network has decreased, which would indicate a failure somewhere in the network (Svensson - col. 1, lines 44-47).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney, McClung, Bloom, Trucchi and Svensson to obtain the invention as specified in claim 17.

As per claim 33, note that Mooney, McClung, Bloom and Trucchi disclose the monitoring device of claim 16 and a star wiring between the capacitors (50) ***(Bloom - col. 8, lines 47-50: "As shown in Fig. 9, the capacitors and resistors are arranged in what is know of in the electrical art as a "Y" configuration or star configuration.")***.

Mooney, McClung, Bloom and Trucchi do not expressly disclose the monitoring device with the alarm detection means (46) is connected, remote from the data

processing system (2), to the individual lines (4a-d) of the network connection (4) by a star wiring between the capacitors (50).

Svensson discloses an alarm detection means is connected, remote from the data processing system, to the individual lines of the network connection ***(Svensson – Fig. 7: Alarm Center '1' is connected, remote from the PC '13a', to the individual line coupled to Hub '3' to individual line toward Network Board '30')***.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Svensson's alarm detection connected to a network connection in Mooney, McClung, Bloom and Trucchi's monitoring device with a star wiring between the capacitors to improve the apparatus with reasonable expectation that this would result in a monitoring device that could use an alarm device to detect whether the network is intact or whether the loading in the network has decreased, which would indicate a failure somewhere in the network (Svensson - col. 1, lines 44-47).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney, McClung, Bloom, Trucchi and Svensson to obtain the invention as specified in claim 33.

14. **Claim 22** is rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of Svensson, and further in view of Lam et al. (4,287,513) hereinafter referred to as Lam. **As per claim 22**, note that Mooney and Svensson disclose the monitoring device of claim 21, and the network connection ***(Svensson – Fig. 7: Network Board '30')***.

Mooney and Svensson do not expressly disclose the alarm detection is effected by monitoring a rest current applied to the alarm circuits (28, 30, 32, 34, 36, 38).

Lam discloses the alarm detection is effected by monitoring a rest current applied to the alarm circuits ***(Lam – col. 7, lines 54-58: "When the alarm circuit is in its quiescent state, the pulses appearing at the input '801' to the detection circuit '80' are large enough to raise the potential of the output '803' to a level above the potential at the node '822', thereby rendering the transistor '820' non-conductive.").***

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Lam's alarm detection monitoring a rest current in Mooney and Svensson's monitoring device to improve the apparatus with reasonable expectation that this would result in the alarm not activating because the transistor disables the tone generator circuit due to no current flow (Lam - col. 7, lines 59-63).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney, Svensson and Lam to obtain the invention as specified in claim 22.

15. **Claim *23*** is rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of McClung, and further in view of Glenn (5,406,261) hereinafter referred to as Glenn. **As per claim 23**, note that Mooney and McClung disclose the monitoring device of claim 8.

Mooney and McClung do not expressly disclose an alarm triggered causes a device, e.g. a bolt gun, to mechanically destroy at least one access-protected data carrier of the data processing system (2).

Glenn discloses an alarm triggered causes a device, e.g. a bolt gun, to mechanically destroy at least one access-protected data carrier of the data processing

system ***(Glenn - col. 9, lines, 41-42: "a microexplosive device for destroying the computer system memory storage device")***.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Glenn's microexplosive device in Mooney and Svensson's monitoring device having a device to mechanically destroy a data carrier to improve the apparatus with reasonable expectation that this would result in an easily operable means to prevent theft and unauthorized operation or handling of the computer system and access of data contained in it.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney, McClung and Glenn to obtain the invention as specified in claim 23.

As per claim 24, note that Mooney and McClung disclose the monitoring device of claim 8.

Mooney and McClung do not expressly disclose a circuit for triggering the alarm manually, e.g. with a manual switch, is provided at least one of the alarm circuits (28, 30, 32, 34, 36, 38).

Glenn discloses a circuit for triggering the alarm manually, e.g. with a manual switch, is provided at least one of the alarm circuits ***(Glenn – col. 10, lines 17-19: "a wireless remote control transmitter and receiver system having a plurality of coded signals for controlling said power switch and alarm states")***.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Glenn's manual switch in Mooney and McClung's monitoring device to trigger the alarm to improve the apparatus with reasonable expectation that this would

result in an easily operable means to prevent theft and unauthorized operation or handling of the computer system and access of data contained in it.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney, McClung and Glenn to obtain the invention as specified in claim 24.

16. **Claims 29 and 36** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of Svensson, and further in view of Glenn.

As per claim 29, note that Mooney and Svensson disclose the method of claim 28.

Mooney and Svensson do not expressly disclose the alarm can be triggered manually, e.g. by means of a switch.

Glenn discloses the alarm can be triggered manually, e.g. by means of a switch ***(Glenn – col. 10, lines 17-19: "a wireless remote control transmitter and receiver system having a plurality of coded signals for controlling said power switch and alarm states")***.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Glenn's manual switch in Mooney and Svensson's monitoring device to trigger the alarm to improve the apparatus with reasonable expectation that this would result in an easily operable means to prevent theft and unauthorized operation or handling of the computer system and access of data contained in it.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney, Svensson and Glenn to obtain the invention as specified in claim 29.

As per claim 36, Mooney and Glenn disclose the method of claim 29, characterized in that a mechanical destruction of at least one access-protected data carrier of the data processing system (2) ***(Glenn - col. 9, lines, 41-42: "a microexplosive device for destroying the computer system memory storage device")*** is caused by an alarm triggered ***(Glenn – col. 2, line 49: "enabling an alarm")***.

17. **Claim *34*** is rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of McClung, in view of Bloom, in view of Trucchi, in view of Svensson, and further in view of Svensson, and further in view of Lam.

As per claim 34, note Mooney, McClung, Bloom, Trucchi and Svensson disclose the monitoring device of claim 17 and the network connection (4) ***(Svensson – Fig. 7: Network Board '30')***.

Mooney, McClung, Bloom, Trucchi and Svensson do not expressly disclose the alarm detection is effected by monitoring a rest current applied to the alarm circuits (28, 30, 32, 34, 36, 38).

Lam discloses the alarm detection is effected by monitoring a rest current applied to the alarm circuits ***(Lam – col. 7, lines 54-58: "When the alarm circuit is in its quiescent state, the pulses appearing at the input '801' to the detection circuit '80' are large enough to raise the potential of the output '803' to a level above the potential at the node '822', thereby rendering the transistor '820' non-conductive.").***

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to Lam's alarm detection monitoring a rest current in Mooney, McClung, Bloom, Trucchi and Svensson's monitoring device to improve the apparatus with

reasonable expectation that this would result in the alarm not activating because the transistor disables the tone generator circuit due to no current flow (Lam - col. 7, lines 59-63).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Mooney, McClung, Bloom, Trucchi, Svensson and Lam to obtain the invention as specified in claim 34.

Allowable Subject Matter

18. **Claims 14, 18 and 19** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAYTON LEWIS-TAYLOR whose telephone number is (571)270-7754. The examiner can normally be reached on Monday through Thursday, 8AM TO 4PM, EASTERN TIME.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tariq Hafiz can be reached on 571-272-6729. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/DAYTON LEWIS-TAYLOR/
Examiner, Art Unit 2182
07/30/2009

/Tariq Hafiz/
Supervisory Patent Examiner, Art Unit 2182